

ESD ACCESSION LIST

DRI Call No. 83512Copy No. 1 of 2 cys.

FILE COPY

Technical Note

1975-50

The Use of Finite Fields
and Rings
to Compute Convolutions

I. S. Reed

6 June 1975

Prepared for the Advanced Research Projects Agency
under Electronic Systems Division Contract F19628-73-C-0002 by

Lincoln Laboratory

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

LEXINGTON, MASSACHUSETTS



Approved for public release; distribution unlimited.

ADA D116955

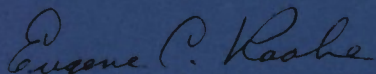
The work reported in this document was performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology. This work was sponsored by the Advanced Research Projects Agency of the Department of Defense under Air Force Contract F19628-73-C-0002 (ARPA Order 2006).

This report may be reproduced to satisfy needs of U.S. Government agencies.

The views and conclusions contained in this document are those of the contractor and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency of the United States Government.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER



Eugene C. Raabe, Lt. Col., USAF
Chief, ESD Lincoln Laboratory Project Office

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

THE USE OF FINITE FIELDS
AND RINGS TO COMPUTE CONVOLUTIONS

I. S. REED

Group 24

TECHNICAL NOTE 1975-50

6 JUNE 1975

Approved for public release; distribution unlimited.

LEXINGTON

MASSACHUSETTS

ABSTRACT

This note extends briefly the integer transforms of C.M. Rader (1972) to transforms over finite fields and rings. These transforms have direct application to digital filters and make possible digital filtering without round-off error. In some cases, the parameters of such number-theoretic transforms can be chosen so that substantial reductions in hardware are possible over what would be needed using classical digital filtering techniques.

CONTENTS

Abstract	iii
Summary	vi
I. Introduction	1
II. DFT on a Galois Field	1
III. Integer Arithmetic Preserving Finite Field Transforms	8
IV. Transforms in Modular Arithmetic and Modulo m Rings	13
References	18

SUMMARY

This note reports briefly on material found for utilizing finite fields and rings to compute convolutions of finite sequences of integers. The methods described generalize the integer transform methods of Rader¹ to similar transforms over finite fields and rings.

Some fundamentals of finite or Galois fields $GF(p^n)$ are informally introduced. Then, following Pollard,² d -point Fourier-like transforms are defined and shown to be the only linear transforms in $GF(p^n)$ with the circular convolution property. This generalizes to Galois fields a result due to Agarwal and Burrus³ for the convolution of integer sequences.

Since the set $G(p)$ of integers modulo a prime number p is always a subfield of $GF(p^n)$, d -point transforms over $GF(p^n)$ can be utilized to compute the transform of a sequence of integers $\{a_1, a_2, \dots, a_d\}$ where a_n lies in the range $-[(p-1)/2] \leq a_n \leq (p-1)/2$. As a consequence, the circular convolution of two such sequences can be computed using d -point transforms over $GF(p^n)$.

An interesting special case occurs if $n = 2$ and q is a Mersenne prime of form $q = 2^p - 1$, where p is a prime. For this case, $GF(q^2)$ is shown to mimic the complex numbers. That is, all elements of $GF(q^2)$ are of the form $a + \hat{i}b$ where $a, b \in GF(q)$, and \hat{i} satisfy the equations $x^2 + 1 = 0$.

The d -point transforms of $GF(q^2)$ are shown to be candidates for computing convolutions of two sequences of complex integers. Since d , the number of points in the transform, must divide the order $q^2 - 1 = 2^{p+1}(2^{p-1} - 1)$ of the multiplicity subgroup of $GF(p^2)$, the number of points in a transform over $GF(q^2)$ can be chosen to be a power of 2. Thus one can utilize the fast Fourier transform (FFT) algorithm to compute convolutions of complex numbers without round-off error.

In the last section of this note, a theorem, stated by Pollard² on transforms over a ring of integers modulo m , is examined. This leads to the notion of the modular arithmetic transform. The Chinese remainder theorem is used to map modular arithmetic transforms into the transforms of integers modulo m .

THE USE OF FINITE FIELDS AND RINGS TO COMPUTE CONVOLUTIONS

I. INTRODUCTION

Recently C. M. Rader showed in Ref. 1 that the convolution of two finite sequences of integers (a_k) and (b_k) for $k = 1, 2, \dots, d$ can be obtained as the inverse transform of the product of two transforms which were other than the usual discrete Fourier transform (DFT). Rader defined transforms of the form

$$A_k \equiv \sum_{n=0}^{d-1} a_n 2^{nk} \text{ Mod } b \quad (1)$$

where b was either a Mersenne number

$$b = 2^p - 1, \quad p \text{ a prime},$$

or b was the Fermat number

$$b = 1 + 2^{2^m}, \quad m \text{ an integer}.$$

The primary advantage of the above Rader transform over the discrete Fourier transform,

$$F_k = \sum_{n=0}^{d-1} a_n w^{nk}, \quad (2)$$

where w is a d^{th} root of unity, lies in the fact that the multiplications by powers of w are replaced in binary arithmetic by simple shifts. Of course, this advantage must be weighed against the difficulties of computing the answer modulo b and of the numeric constraints, relating word length, length of sequence d and compositeness of d , imposed by the above two choices for b , suggested by Rader. Our purpose here is to review the Rader transform first by enlarging the class of transforms, given by (1), and second by presenting more details of the computational algorithm for computing such a convolution with (1).

In the next section, the class of transforms given by (1) is increased to include a Fourier-type transform over an arbitrary finite field, the Galois field. Such a generalization has been discussed recently by J. M. Pollard² in 1974, but also much earlier by Reed and Solomon³ in 1959 in a somewhat different context. The approach used here will follow the more explicit approach of the earlier reference.

II. DFT ON A GALOIS FIELD

The only finite fields are the Galois fields. The number of elements in a Galois field is p^n where p is a prime number and n is a positive integer. To construct a Galois field $GF(p^n)$, one must first find an n^{th} degree polynomial $p(x)$ over $GF(p)$ which is irreducible. The elements of $GF(p^n)$ are then all polynomials of the form

$$f(\alpha) = \sum_{i=0}^{n-1} f_i \alpha^i, \quad f_i \in GF(p), \quad (i = 0, 1, 2, \dots, n-1)$$

where α is a root of $p(x)$, i.e., $p(\alpha) = 0$. The product $h(\alpha)$ of two elements say $f(\alpha)$ and $g(\alpha)$ in $GF(p^n)$ is the residue of $f(x)g(x)$ modulo $p(x)$ with α substituted for x . That is, $h(\alpha)$ is found by

$$h(x) \equiv f(x)g(x) \text{ Mod } p(x)$$

where $x = \alpha$. Similarly, the sum $s(\alpha)$ is found by

$$s(x) \equiv f(x) + g(x) \text{ Mod } p(x)$$

where $x = \alpha$. By taking the sums and products of all polynomials $f(\alpha)$ in this manner, the addition and multiplication tables of the elements of $GF(p^n)$ can be found. Let this be illustrated by the following example.

Example 1

Consider the integers modulo 3. This is the prime field or $GF(3) = \{0, 1, 2\}$ where $2 = -1$. Let

$$p(x) = x^2 + x + 2 \quad .$$

Since $p(0) = 2$, $p(1) = 1$, and $p(2) = 2$, $p(x)$ is irreducible over the coefficient field $GF(3)$. A root to $p(x) = 0$ can only be found in some field containing $GF(3)$, some extension field. If α is such a root, then α satisfies

$$p(\alpha) = \alpha^2 + \alpha + 2 = 0 \quad .$$

Starting with the element α , one computes α^2 by computing $x^2 \text{ Mod } p(x)$ as follows:

$$x^2 + x + 2 \overline{\begin{array}{r} 1 \\ x^2 \\ \underline{x^2 + x + 2} \\ -x - 2 \end{array}} \quad .$$

This $-x - 2 = 2x + 1$ is the residue of $x^2 + x + 2$, and

$$\alpha^2 = 2\alpha + 1$$

is the reduced expression for α^2 . Similarly, one can compute α^3 by computing the residue of $(x)(x^2) = (x)(2x + 1) = 2x^2 + x$, i.e.,

$$x^2 + x + 2 \overline{\begin{array}{r} 2 \\ 2x^2 + x \\ \underline{2x^2 + 2x + 1} \\ -x + 2 \end{array}}$$

Thus

$$\alpha^3 = 2\alpha + 2 \quad .$$

Continuing in this manner one gets the results shown in Table 1.

TABLE 1 THE NON-ZERO ELEMENTS OF $GF(3^2)$							
α	α^2	α^3	α^4	α^5	α^6	α^7	α^8
α	$2\alpha + 1$	$2\alpha + 2$	2	2α	$\alpha + 2$	$\alpha + 1$	1

In this particular case, α and its powers α^i (for $i = 1, 2, \dots, 8$) generate the eight non-zero elements of $\text{GF}(3^2)$. If an element α and its powers generate the non-zero elements of a field, α is called a primitive element. If α is a primitive element, and a root of $p(x)$, which it is in this example, then the relation $p(\alpha) = 0$ can be used to compute the non-zero elements of $\text{GF}(p^n)$. This is done for this example as follows: $p(\alpha) = 0$ is the relation $\alpha^2 + \alpha + 2 = 0$. Solving for α^2 , yields

$$\alpha^2 = 2\alpha + 1 \quad .$$

Then

$$\begin{aligned} \alpha^3 &= \alpha(\alpha^2) = \alpha(2\alpha + 1) = 2\alpha^2 + \alpha \\ &= 2(2\alpha + 1) + \alpha = 2\alpha + 2 \quad , \end{aligned}$$

and so forth, thereby obtaining Table 1.

The above example illustrates the following facts about a Galois field. All the elements of $\text{GF}(p^n)$ satisfy the equation

$$x^{p^n} = x \quad . \quad (3)$$

There exists a primitive element $\alpha \in \text{GF}(p^n)$ which generates the non-zero elements of $\text{GF}(p^n)$. The non-zero elements $\text{GF}(p^n)$ compose a cyclic group.

In general, there always exists an $\alpha \in \text{GF}(p^n)$ such that $\text{GF}(p^n)$ is the set $\{0, \alpha, \alpha^2, \dots, \alpha^{p^n-2}, \alpha^{p^n-1}\}$. α is called $(p^n - 1)$ -th root of unity.

If in (1), b is a prime p , then the Rader transform¹ can be regarded as a mapping of a subset of $\text{GF}(p)$ into $\text{GF}(p)$. To see this, consider the mapping

$$A(x) \equiv \sum_{k=0}^{d-1} a_k x^k \text{ Mod } p \quad . \quad (4)$$

Then the elements of the subset

$$\{1, 2, 2^2, \dots, 2^{d-1}\} \text{ Mod } p$$

of $\text{GF}(p)$ have, successively, the images

$$\{A(1), A(2), A(2^2), \dots, A(2^{d-1})\} \text{ Mod } p \quad ,$$

also a subset of $\text{GF}(p)$ where $a_k \in \text{GF}(p)$. Hence, $A(x)$ as given by (4) is a mapping of a subset of $\text{GF}(p)$ into $\text{GF}(p)$. $A(x)$ is called a polynomial mapping.

More generally, let a_n and x be elements of an arbitrary Galois field, say $\text{GF}(p^n)$, and consider the mapping of subset of d distinct non-zero elements

$$\Theta_d = \{\tau_0, \tau_1, \dots, \tau_{d-1}\} \quad \tau_k \in \text{GF}(p^n)$$

into $\text{GF}(p^n)$ with the polynomial mapping

$$A(x) = \sum_{k=0}^{d-1} a_k x^k \quad . \quad (5)$$

This is the most general possible mapping of $GF(p^n)$ into $GF(p^n)$ (see Ref. 3). This mapping can be displayed as a system of linear equations in the coefficients a_τ as follows.

$$\begin{aligned}
 A(\tau_1) &= a_0 + a_1\tau_1 + a_2\tau_1^2 + \dots a_{d-1}\tau_1^{d-1} \\
 A(\tau_2) &= a_0 + a_1\tau_2 + a_2\tau_2^2 + \dots a_{d-1}\tau_2^{d-1} \\
 &\vdots \\
 A(\tau_d) &= a_0 + a_1\tau_d + a_2\tau_d^2 + \dots a_{d-1}\tau_d^{d-1} \quad .
 \end{aligned} \tag{6}$$

This system can be written further in matrix form as

$$\underline{A} = T \underline{a} \tag{7}$$

where \underline{a} and \underline{A} are the column matrices

$$\underline{a} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{bmatrix} \quad \text{and} \quad \underline{A} = \begin{bmatrix} A(\tau_1) \\ A(\tau_2) \\ \vdots \\ A(\tau_d) \end{bmatrix}$$

and

$$T = \begin{bmatrix} 1 & \tau_1 & \tau_1^2 & \dots & \tau_1^{d-1} \\ 1 & \tau_2 & \tau_2^2 & \dots & \tau_2^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \tau_d & \tau_d^2 & \dots & \tau_d^{d-1} \end{bmatrix}$$

is a $d \times d$ matrix of elements in $GF(p^n)$.

By (7) the polynomial mapping (5) can also be regarded as a linear mapping of the vector \underline{a} onto vector a vector \underline{A} . Such a mapping is one to one or is invertible if matrix T has an inverse, that is, if the determinant $|T|$ of T is non-zero. Since the determinant of T is a Vandermonde determinant, it can be evaluated as

$$|T| = \prod_{j < i} (\tau_i - \tau_j) \neq 0$$

since the τ_j 's are all distinct. Thus T^{-1} exists and (7) can be solved as

$$\underline{a} = T^{-1} \underline{A} \quad ,$$

the inverse "transform."

Next let us impose on (7) the constraint that it can be used to compute circular convolution s_n of sequences a_n and b_n ,

$$S_n = \sum_{k=0}^{d-1} a_k b_{(n-k)} \quad (9)$$

where $(n-k)$ is the residue of $(n-k)$ modulo d . One wants the transform of S_n , namely, \underline{S} to be given by

$$\underline{S} = \begin{bmatrix} S(\tau_1) \\ S(\tau_2) \\ \cdot \\ \cdot \\ S(\tau_d) \end{bmatrix} = \begin{bmatrix} A(\tau_1) & \cdot & B(\tau_1) \\ A(\tau_2) & \cdot & B(\tau_2) \\ \cdot & & \cdot \\ \cdot & & \cdot \\ A(\tau_d) & \cdot & B(\tau_d) \end{bmatrix} = \underline{A} \otimes \underline{B} \quad .$$

Equating components

$$S(\tau_k) = A(\tau_k) B(\tau_k) \quad \text{for } k = 1, 2, \dots, d$$

or

$$\sum_{n=0}^{d-1} s_n \tau_k^n = \sum_{\ell=0}^{d-1} \sum_{m=0}^{d-1} a_\ell b_m \tau_k^{\ell+m} \quad .$$

Substituting (9) in the left side,

$$\sum_{n=0}^{d-1} \sum_{p=0}^{d-1} a_p b_{(n-p)} \tau_k^n = \sum_{\ell=0}^{d-1} \sum_{m=0}^{d-1} a_\ell b_m \tau_k^{\ell+m} \quad .$$

Next if one substitutes ℓ for p and m for residue of $(n-p)$ Mod d in the left side, then

$$\sum_{\ell=0}^{d-1} \sum_{m=0}^{d-1} a_\ell b_m \tau_k^{(m+\ell)} = \sum_{\ell=0}^{d-1} \sum_{m=0}^{d-1} a_\ell b_m \tau_k^{\ell+m} \quad .$$

Finally, equating coefficients of $a_\ell b_m$, one gets

$$\tau_k^{(m+\ell)} = \tau_k^{\ell+m} \quad (10)$$

for $(k, \ell, m = 0, 1, 2, \dots, d-1)$ where $(m+\ell)$ is the residue of $(m+\ell)$ modulo d .

In order to satisfy (10), suppose $m+\ell$ is an integer r in the interval $d \leq r < 2d$, then

$$m+\ell = r = d + (r)$$

where (r) is the residue. In this notation (10) becomes

$$\tau_k^{(r)} = \tau_k^{d+(r)} = \tau_k^d \cdot \tau_k^{(r)} \quad (11)$$

Since by assumption $\tau_k \neq 0$, the inverse element $[\tau_k^{(r)}]^{-1}$ in $\text{GF}(p^n)$ of $\tau_k^{(r)}$ exists. Multiplying both sides of (11) by this inverse yields

$$\tau_k^d = 1 \quad \text{for } k = 1, 2, \dots, d \quad . \quad (12)$$

That is, for transform (7) to yield circular convolutions, τ_k must be a d^{th} root of unity for $k = 1, 2, \dots, d$ in $\text{GF}(p^n)$. This is essentially the same result Agarwal and Burrus got in Ref. 4 for the circular convolution of integer sequences.

Since the non-zero elements of $\text{GF}(p^n)$ form a cyclic group of order $p^n - 1$, the truth of (12) for an element $\tau_k \in \text{GF}(p^n)$ implies integer d divides $p^n - 1$. That is, $d | p^n - 1$ if transform (7) is to yield a circular convolution. Moreover, since the set of elements $(\tau_1, \tau_2, \dots, \tau_d)$ are distinct and are all d^{th} roots of unity, this set must be a cyclic subgroup of the cyclic subgroup of the non-zero elements of $\text{GF}(p^n)$. Thus the set, $(\tau_1, \tau_2, \dots, \tau_d)$, equals the subgroup $(\alpha, \alpha^2, \dots, \alpha^{d-1}, 1) = \varphi_d$, i.e.,

$$\{\tau_1, \tau_2, \dots, \tau_d\} = \{\alpha, \alpha^2, \dots, \alpha^{d-1}, 1\} = \varphi_d \quad (13)$$

in some order where $\alpha \in \text{GF}(p^n)$ is a generator of the subgroup.

If the group $\varphi_d = (\alpha, \alpha^2, \dots, \alpha^{d-1}, 1)$ is substituted for $(\tau_1, \tau_2, \dots, \tau_d)$ in transform (7), the transform becomes

$$A_k = \sum_{n=0}^{d-1} a_n \alpha^{kn} \quad \text{for } (k = 0, 1, 2, \dots, d-1) \quad . \quad (14)$$

To invert (14), observe first that all elements of φ_d satisfy the equation

$$x^d - 1 = 0 \quad .$$

But since $x^d - 1$ factors as

$$x^d - 1 = (x - 1) \sum_{n=0}^{d-1} x^n \quad ,$$

one has

$$\begin{aligned} \sum_{k=0}^{d-1} x^k &= 0 \quad \text{for } x \neq 1 \quad \text{and} \quad x \in \varphi_d \subseteq \text{GF}(p^n) \\ \sum_{k=0}^{d-1} x^k &= \underbrace{1 + 1 + \dots + 1}_{d \text{ times}} = (d) \quad \text{for } x = 1 \end{aligned} \quad (15)$$

where (d) denotes the residue of d modulo p . This formula is given by Pollard [Ref. 2, Eq. (8)] and earlier by Reed and Solomon [Ref. 3, Eq. (3)].

From (15) we now derive the discrete "delta" function needed to invert (14). Consider the sum of x^n over all the elements of the multiplicative subgroup φ_d , defined by (13). This is

$$\sum_{x \in \varphi_d} x^n = \sum_{k=0}^{d-1} (\beta^k)^n = \sum_{k=0}^{d-1} (\beta^n)^k \quad .$$

But this is in the form of (15) and β^n is an element of φ_d , thus

$$\begin{aligned} \sum_{x \in \varphi_d} x^n &= \sum_{k=0}^{d-1} (\beta^n)^k = 0 \quad \text{for } n \not\equiv 0 \pmod{d} \\ &= (d) \quad \text{for } n \equiv 0 \pmod{d} \\ &= (d) \delta_d(n) \end{aligned} \tag{16}$$

where $\delta_d(n)$ is the delta function

$$\begin{aligned} \delta_d(n) &= 0 \quad \text{for } n \not\equiv 0 \pmod{d} \\ &= 1 \quad \text{for } n \equiv 0 \pmod{d} \end{aligned}$$

Since (d) is an element of field $\text{GF}(p^n)$, the inverse $(d)^{-1}$ exists in $\text{GF}(p^n)$. Now, multiply A_k by $(d)^{-1} \alpha^{-km}$ and sum on k for $(k = 0, 1, 2, \dots, d-1)$. This yields by (14) and (16),

$$\begin{aligned} (d)^{-1} \sum_{k=0}^{d-1} A_k \alpha^{-km} &= (d)^{-1} \sum_{k=0}^{d-1} \sum_{n=0}^{d-1} a_n \alpha^{kn} \alpha^{-km} \\ &= (d)^{-1} \sum_{n=0}^{d-1} a_n \left(\sum_{k=0}^{d-1} \alpha^{k(n-m)} \right) = (d)^{-1} (d) \sum_{n=0}^{d-1} a_n \delta_d(n-m) \\ &= a_m \end{aligned}$$

Thus,

$$A_k = \sum_{n=0}^{d-1} a_n \alpha^{kn}$$

and

$$a_n = (d)^{-1} \sum_{k=0}^{d-1} A_k \alpha^{-kn} \tag{17}$$

where a_n and A_k are elements of $\text{GF}(p^n)$ and α is a generator of d element subgroup δ_d , the multiplicative subgroup of $\text{GF}(p^n)$.

To show the circular convolution property of (17), let

$$A_k = \sum_{n=0}^{d-1} a_n \alpha^{kn}, \quad B_k = \sum_{m=0}^{d-1} b_m \alpha^{km}$$

and

$$C_k = A_k \cdot B_k$$

Then by (17) the inverse transform of C_k for $(k = 0, 1, \dots, d-1)$ is

$$\begin{aligned}
(d)^{-1} \sum_{k=0}^{d-1} C_k \alpha^{-kp} &= (d)^{-1} \sum_{k=0}^{d-1} \sum_{n=0}^{d-1} \sum_{m=0}^{d-1} a_n b_m \alpha^{k(m+n-p)} \\
&= (d)^{-1} \sum_{n=0}^{d-1} \sum_{m=0}^{d-1} a_n b_m \sum_{k=0}^{d-1} \alpha^{k(m+n-p)} \\
&= \sum_{n=0}^{d-1} \sum_{m=0}^{d-1} a_n b_m \delta_d(n+m-p) = \sum_{n=0}^{d-1} a_n b_{(p-n)} \quad (18)
\end{aligned}$$

where $(p-n)$ denotes the residue of $(p-n)$ modulo d .

The result, given by (18), shows finally that the imposition of condition (12) on the transform, given by (7), is both necessary and sufficient for transform (7) to yield circular convolutions. This generalizes a similar result, given by Agarwal and Burrus in Ref. 4, for the field of complex numbers to all fields both finite and infinite. In the next section, we show how to restrict the finite field transform, given by (17), so that it yields circular convolutions over both the integers and complex integers.

III. INTEGER ARITHMETIC PRESERVING FINITE FIELD TRANSFORMS

Suppose a is an integer of magnitude less than or equal $(p-1)/2$ where p is a prime. Then integer a satisfies

$$-[(p-1)/2] \leq a \leq (p-1)/2.$$

If $a \geq 0$, a is the residue modulo p . If $a = -b$ where $b > 0$, then

$$a \equiv p-b \pmod{p}.$$

Thus the set of positive integers

$$\left\{ -\frac{p-1}{2}, \dots, -2, -1, 0, 1, 2, \dots, \frac{p-1}{2} \right\}$$

corresponds in a one-to-one manner with the following set of residues modulo p ,

$$\left\{ (p - \frac{p-1}{2}), \dots, p-2, p-1, 0, 1, 2, \dots, \frac{p-1}{2} \right\}.$$

Since the latter set exhausts all residues modulo p , this set uniquely represents the set of all positive and negative real integers of magnitude less than or equal to $(p-1)/2$, namely, the set $\{x \mid |x| \leq (p-1)/2\}$, x a positive or negative integer. However, the set of residues modulo p composes precisely the Galois or finite field $GF(p)$, hence the above correspondence maps the set of integers less than or equal to $(p-1)/2$ onto $GF(p)$ in a one-to-one manner.

In order to carry out arithmetic operations in $GF(p)$ which arrive at the correct arithmetic answer, one must often restrict the operating ranges of the integer variables even further. For example, to compute the circular convolution (18) in $GF(p)$ where a_n and b_n are integers, one requires the final convolution to lie in the same "dynamic range" as the integers a_n and b_n . That is, in order to avoid ambiguity

$$-\frac{p-1}{2} \leq \sum_{n=0}^{d-1} a_n b_{(p-n)} \leq \frac{p-1}{2}$$

or its equivalent

$$\left| \sum_{n=0}^{d-1} a_n b_{(p-n)} \right| \leq \frac{p-1}{2} \quad (19)$$

Since

$$\left| \sum_{n=0}^{d-1} a_n b_{(p-n)} \right| \leq \sum_{n=0}^{d-1} |a_n| |b_{(p-n)}|$$

where equality holds, if a_n and b_n are positive integers, to satisfy (19) for all sequences a_n and b_n such that $|a_n| \leq A$ and $|b_n| \leq B$, it is necessary that

$$\sum_{n=0}^{d-1} (\text{Max } |a_n|) [\text{Max } |b_{(p-n)}|] = dAB \leq \frac{p-1}{2} \quad (20)$$

A and B are the dynamic or operating ranges of integers, $|a_n|$ and $|b_n|$, respectively. If $A = B$, then by (20) the largest value of A is given by

$$A = \left\lfloor \sqrt{\frac{p-1}{2d}} \right\rfloor \quad (21)$$

where $\lfloor x \rfloor$ denotes greatest integer less than x , what is often called the principle part of x .

Assuming (21), which for many practical applications is somewhat pessimistic, one would need to constrain a_n and b_n to the interval.

$$-A = -\left\lfloor \sqrt{\frac{p-1}{2d}} \right\rfloor \leq a_n, b_n \leq \left\lfloor \sqrt{\frac{p-1}{2d}} \right\rfloor = A \quad (22)$$

in order to compute the circular convolution

$$C_p = \sum_{n=0}^{d-1} a_n b_{(p-n)} \quad (23)$$

unambiguously with modulo p arithmetic, i.e., keep c_n in the interval

$$-\frac{p-1}{2} \leq c_n \leq \frac{p-1}{2} \quad .$$

To compute convolution (23) when a_n and b_n are integers in a Galois field with transforms of the type suggested by Rader [Eq. (1)], one must first represent the integers in such a field. To preserve the arithmetic operations of addition and multiplication, the representation must necessarily be restricted to $GF(p)$ in the manner shown above. However, $GF(p)$ is a subfield of $GF(p^n)$; in fact, the ground field of $GF(p^n)$ for all n ($n = 1, 2, 3, \dots$). Thus, convolution (23) can be performed with transforms of type (17) on a Galois field $GF(p^n)$ if a_n and b_n are restricted to $GF(p)$. In others words, if $a_n, b_n \in GF(p)$ for $(n = 0, 1, 2, \dots, d-1)$ and the transforms are

$$A_k = \sum_{n=0}^{d-1} a_n \alpha^{kn} \quad \text{and} \quad B_k = \sum_{n=0}^{d-1} a_n \alpha^{kn} \quad \text{for } (k = 0, 1, \dots, d-1)$$

where α is a generator of a d -element subgroup φ_d of $[\text{GF}(p^n) - 0]$, then the d -point convolution

$$C_p = \sum_{n=0}^{d-1} a_n b_{(p-n)}$$

if integers a_n and b_n is found by forming

$$C_k = A_k \cdot B_k \quad \text{for } (k = 0, 1, \dots, d-1)$$

and then taking the inverse transform

$$C_n = (d)^{-1} \sum_{k=0}^{d-1} C_k \alpha^{-kn}.$$

If an α can be found so that multiplications by powers of α are simple in hardware, the above extension might be useful in increasing the number of possible points in the convolution. This follows from the fact that d is a divisor of $p^n - 1$ and the number of divisors of $p^n - 1$ is always greater than the number of divisors of $p - 1$.

In applications to radar and communications systems, one generally wants to take convolutions of complex numbers. Towards this end set $a_n = \alpha_n + i\beta_n$ and $b_n = x_n + iy_n$ where α_n, β_n, x_n , and y_n are integers, suitably restricted in $\text{GF}(P)$ so that the real and imaginary parts of

$$C_p = \sum_{n=0}^{d-1} a_n b_{(p-n)} = \gamma_n + i\delta_n \quad (24)$$

lie in the interval $-[(p-1)/2] \leq \gamma_n, \delta_n \leq (p-1)/2$ for $(n = 0, 1, \dots, d-1)$

$$a_n b_n = \alpha_n x_n - \beta_n y_n + i(\alpha_n y_n + \beta_n x_n).$$

Thus one needs four transforms, A_k, B_k, X_k , and Y_k of α_n, β_n, x_n , and y_n , respectively, as well as four inverse transforms of the products,

$$A_k X_k, B_k Y_k, A_k Y_k, B_k X_k \quad (25)$$

to find (24), the circular convolution of complex integers. It is of interest to note that, for certain prime numbers q , this computational requirement can be reduced from four to two Rader-type transforms.

To achieve this, prime q must be such that

$$X^2 \equiv -1 \pmod{q} \quad (26)$$

is not solvable. But the non-solvability of (26) is the same as the statement, (-1) is a quadratic nonresidue (Ref. 5, p. 82). This is further equivalent to

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$$

where (a/q) is the Legendre symbol, defined by

$$\begin{aligned} \frac{a}{q} &= +1 & \text{if } a \text{ is quadratic residue Mod } q \\ &= -1 & \text{if } a \text{ is quadratic nonresidue Mod } q. \end{aligned}$$

There are two important special cases.

Case I.

Mersenne primes of form $M_p = 2^p - 1$ where p is prime. For this case

$$\begin{aligned} \left(\frac{-1}{M_p}\right) &= (-1)^{(M_p-1)/2} = (-1)^{(2^p-2)/2} \\ &= (-1)^{(2^{p-1}-1)} = -1 \end{aligned}$$

Thus (-1) is a quadratic nonresidue and (26) is not solvable, modulo M_p .

Case II.

Fermat primes of form $F_m = 2^{2^m} + 1$ for $1 \leq m \leq 4$. For this case

$$\left(\frac{-1}{F_m}\right) = (-1)^{(F_m-1)/2} = (-1)^{2^{2^m-1}} = +1$$

Thus (-1) is a quadratic residue modulo F_m and (26) is solvable.

If (26) is not solvable, which is true when q is a Mersenne prime $M_p = 2^p - 1$, then polynomial

$$P(x) = x^2 + 1$$

is irreducible in $GF(q)$. By the procedure of the last section (see Example 1) a root, say \hat{i} , of

$$P(x) = x^2 + 1 = 0 \tag{27}$$

can be found in the extension field $GF(q^2)$. $GF(q^2)$ is composed of the set

$$GF(q^2) = \{a + \hat{i}b \mid a, b \in GF(q)\} \tag{28}$$

where \hat{i} is a root of (27), satisfying

$$\hat{i}^2 = -1 \tag{29}$$

where $-1 \equiv (q-1) \pmod{q}$.

Evidently \hat{i} plays a similar role over the finite field $GF(q)$ that $\sqrt{-1} = i$ plays over the field of rational numbers. For example, suppose $a + \hat{i}b$ and $c + \hat{i}d$ are elements of $GF(q^2)$, then by (29)

$$(a + \hat{i}b) \pm (c + \hat{i}d) = (a \pm c) + \hat{i}(b \pm d)$$

and

$$\begin{aligned} (a + \hat{i}b)(c + \hat{i}d) &= ac + \hat{i}^2bd + \hat{i}bc + \hat{i}ad \\ &= ac - bd + \hat{i}(bc + ad) \end{aligned}$$

the exact analogues of what one might expect if $a + \hat{i}b$ and $c + \hat{i}d$ were complex numbers. Thus if -1 is a quadratic nonresidue mod q , then the circular convolution (24) of the complex integers, a_n and b_n , can be computed, using only two inverse transforms on the terms

$$A_k X_k - B_k Y_k, A_k Y_k + B_k X_k$$

defined in (25).

In the next section we will show how the transforms, developed by Rader for prime fields and extended here to Galois fields, can be extended further to rings, formed from these fields. Before doing this, however, it is of some independent interest to demonstrate one property of the Galois field $GF(q^2)$ which the field of complex rational numbers does not have. If $x = a + \hat{i}b \in GF(q^2)$, $x \neq 0$, then

$$x^{q^2-1} = (a + \hat{i}b)^{q^2-1} = 1 \quad .$$

A true complex number does not have this property.

To prove this, use the binomial theorem

$$(a + \hat{i}b)^{q^2-1} = \sum_{k=0}^{q^2-1} \binom{q^2-1}{k} (\hat{i}b)^k a^{q^2-1-k} \quad .$$

But

$$a^{q^2-1} = (a^{q-1})^{q+1} \quad \text{and} \quad a^{q-1} \equiv 1 \pmod{q}$$

so that

$$a^{q^2-1} \equiv 1 \pmod{q} \quad .$$

Also the binomial coefficient is

$$\begin{aligned} \binom{q^2-1}{k} &= \frac{(q^2-1)(q^2-2)\dots(q^2-k)}{1 \cdot 2 \cdot 3 \dots k} \\ &\equiv \frac{[q(q-1) + (q-1)][q(q-1) + (q-2)] \dots [q(q-1) + (q-k)]}{1 \cdot 2 \cdot 3 \dots k} \\ &\equiv \frac{(q-1)(q-2)\dots(q-k)}{1 \cdot 2 \cdot 3 \dots k} \equiv \frac{(-1)(-2)\dots(-k)}{1 \cdot 2 \dots k} \\ &\equiv (-1)^k \pmod{q} \quad . \end{aligned}$$

Thus

$$\begin{aligned} (a + \hat{i}b)^{q^2-1} &= \sum_{k=1}^{q^2-1} (-1)^k (\hat{i}b/a)^k \\ &= \frac{1 - (-\hat{i}b/a)^{q^2}}{1 + \hat{i}b/a} \quad . \end{aligned}$$

However,

$$\begin{aligned} \hat{i}^{q^2} &= \hat{i}^{q^2-1} \hat{i} = (\hat{i}^{q-1})^{q+1} \hat{i} \\ &= [(-1)^{(q-1)/2}]^{q+1} \hat{i} = \left(\frac{-1}{q}\right)^{q+1} \hat{i} \end{aligned}$$

where $\left(\frac{a}{q}\right)$ is the Legendre symbol. But by assumption (-1) is a quadratic nonresidue and $\left(\frac{-1}{q}\right) = -1$. Hence,

$$\hat{i}q^2 = \hat{i}$$

so that finally

$$(a + \hat{i}b)q^2 - 1 = \frac{1 + \hat{i}(b/a)q^2}{i + \hat{i}b/a} = \frac{1 + \hat{i}b/a}{1 + \hat{i}b/a} = 1.$$

We see above that the Mersenne primes M_p have an advantage over the Fermat primes F_m in the computation of convolutions of complex integers. However, as Rader points out in Ref. 1, this advantage must be weighed against the fact that the fast Fourier transform (FFT) algorithm can be applied to the transforms, using Fermat primes, but not to the Mersenne primes.

IV. TRANSFORMS IN MODULAR ARITHMETIC AND MODULO m RINGS

A transform in the ring of integers modulo m was considered by Pollard in Ref. 2. It is well known⁵ that the set of integers modulo m is a ring R_m with respect to addition and multiplication modulo m .

Pollard considered first rings where m was a power of a prime p , namely, $m = p^n$, $p > 0$. He let R_m^* denote the set of elements of R_m prime to m , i.e.,

$$R_m^* = \{a \in R_m \mid (a, m) = 1\}$$

where (a, m) denotes the greatest common divisor of integers a and m .

By Euler's theorem (Ref. 5, p. 48), if $(a, m) = 1$

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad (30)$$

where $\varphi(m)$ denotes the number of divisors of m less than or equal to m , Euler's function. Thus, since 1 is the multiplicative identity of R_m , then

$$a^{\varphi(m)} = 1 \quad (31)$$

for all $a \in R_m^*$.

The order of an element a in R_m (called the exponent of a in number theory) is the least power $e(a)$ such that

$$a^{e(a)} = 1.$$

Also, if $m = p^n$ the number of elements in R_m prime to m is

$$\varphi(m) = p^n - p = p^{n-1}(p-1).$$

Thus by (31) the order of each element $a \in R_m^*$ divides $\varphi(m) = p^{n-1}(p-1)$, i.e., $e(a) \mid p^{n-1}(p-1)$ all $a \in R_m^*$.

It is well known (Ref. 5, p. 107) that an element $g \in R_m^*$ can be found such that $e(g) = p^{n-1}(p-1)$. g is called a primitive root since

$$g^{\varphi(m)} \equiv 1 \pmod{m}$$

and $\varphi(m) = e(g)$ the order or exponent with g belongs to modulo m . The powers of g , that is the set

$$G = \{g, g^2, \dots, g^{p^{n-1}(p-1)}\}$$

are all distinct. Suppose otherwise that

$$g^k = g^\ell, \quad k > \ell$$

where

$$g^k, g^\ell \in G,$$

then

$$g^k \cdot g^{p^{n-1}(p-1)-\ell} = g^{k-\ell} = 1.$$

But $k - \ell < p^{n-1}(p-1) = e(g)$ which is contrary to the assumption that g is a primitive root. Hence the elements of G are distinct. Since the elements of G are prime to $m = p^n$ and since G has the same number of elements as R_m^* ,

$$G = R_m^*.$$

Thus R_m^* is a cyclic multiplication group of $p^{n-1}(p-1)$ elements with generator g .

Pollard next chooses a divisor d of $p-1$ and considers an element $r \in R_m^*$ of order d , i.e., d is the smallest integer for which $r^d = 1$. The powers of r compose a subgroup G_d of R_m^* ,

$$G_d = \{1, r, r^2, \dots, r^{d-1}\}.$$

He next shows that the equivalent of (16) holds when φ_d is replaced by G_d . That is, if $d \mid p-1$,

$$\begin{aligned} \sum_{X \in G_d} X^m &= \sum_{k=0}^{d-1} (r^m)^k = 0 \quad \text{for } m \not\equiv 0 \pmod{d} \\ &= (d) \quad \text{for } m \equiv 0 \pmod{d} \\ &= (d) \delta_d(m) \end{aligned} \tag{32}$$

where $\delta_d(m)$ is the delta function

$$\begin{aligned} \delta_d(m) &= 0 \quad \text{for } m \not\equiv 0 \pmod{d} \\ &= 1 \quad \text{for } m \equiv 0 \pmod{d} \end{aligned}$$

and where (d) is d modulo p^n .

To prove this, consider first the following cyclic subgroup of R_m^*

$$\{g^{p-1}, (g^{p-1})^2, \dots, (g^{p-1})^{p^{n-1}}\} = G_{p^{n-1}} \tag{33}$$

of p^{n-1} elements. By Fermat's theorem [Eq. (31) for m a prime], an element $g^{(p-1)k}$ of $G_{p^{n-1}}$ satisfies

$$(g^{p-1})^k \equiv 1^k \equiv 1 \pmod{p}.$$

However, if we consider an arbitrary element of subgroup,

$$G_{p-1} = \left\{ g^{p^{n-1}}, \left(g^{p^{n-1}} \right)^2, \dots, \left(g^{p^{n-1}} \right)^{p-1} \right\} \quad (34)$$

modulo p , then

$$g^{p^{n-1}k} \equiv \left[\left(\dots \left((g^p)^p \dots \right)^p \right)^{p^{n-1}} \right]^k \equiv \left[\left(\dots (g^p) \dots \right)^p \right]^k \equiv g^k \pmod{p} \quad (35)$$

Since integers $p-1$ and p^{n-1} are relatively prime, i.e., $(p-1, p^{n-1}) = 1$, the subgroups $G_{p^{n-1}}$ and G_{p-1} in (33) and (34), respectively, have only the unit element, 1, in common. Also by (33) and (34) every element of R_m^* is to be found in the product of $G_{p^{n-1}}$ and G_{p-1} . Hence R_m^* is the direct product of these two subgroups, i.e.,

$$R_m^* = G_{p-1} \times G_{p^{n-1}}.$$

Thus the only elements of R_m^* which are not congruent to 1 modulo p are the complement of $G_{p^{n-1}}$ and hence in G_{p-1} .

Let h be a primitive root modulo p , i.e., h is an integer $1 < h \leq p-1$ such that $p-1$ is the least integer for which

$$h^{p-1} \equiv 1 \pmod{p}.$$

Then it can be shown (see Ref. 5, p. 107) that a primitive root g modulo p^n can always be found of form

$$g = h + \mu p$$

where μ is an integer. From this

$$g^k \equiv (h + \mu p)^k \equiv h^k \pmod{p}$$

where $1 < h \leq p-1$. With (35) this yields

$$g^{p^{n-1}k} \equiv h^k \pmod{p} \quad (36)$$

Since h is a primitive root modulo p , it generates the $p-1$ element group φ_{p-1} of the non-zero elements of $R_p = GF(p)$. (36) maps the elements of G_{p-1} onto φ_{p-1} in one-to-one manner. Since $g^{p^{n-1}(k+l)} \equiv h^{k+l} \pmod{p}$, this mapping is in fact an isomorphism between groups G_{p-1} and φ_{p-1} , i.e., $G_{p-1} \cong \varphi_{p-1}$.

By (36) if some element of G_{p-1} was congruent to 1 modulo p , then

$$g^{p^{n-1}k} \equiv h^k \equiv 1 \pmod{p}.$$

Since h is primitive this is possible if and only if k is a multiple of $p-1$. Thus none of the elements of G_{p-1} is congruent to 1 modulo p , except the unit element 1. Since $d \mid p-1$, G_d is a cyclic subgroup of G_{p-1} , and likewise no element x , $x \neq 1$, of G_d is congruent to 1 modulo p .

Now for $m \not\equiv 0 \pmod{d}$

$$\left(\sum_{k=0}^{d-1} (r^m)^k \right) (r^m - 1) \equiv (r^d)^m - 1 \equiv (1)^m - 1 \equiv 0 \pmod{p^n} \quad (37)$$

where r is a generator of G_d . From the above, if $m \not\equiv 0 \pmod{d}$,

$$r^m \not\equiv 1 \pmod{p}.$$

Thus, the integer $r^m - 1$ and p are relatively prime ($(r^m - 1, p) = 1$). But this in turn implies $(r^m - 1, p^n) = 1$ for $(m = 1, 2, \dots, d-1)$. Thus

$$\sum_{k=0}^{d-1} (r^m)^k \equiv 0 \pmod{p^n}$$

for all $m \not\equiv 0 \pmod{d}$ and (32) is proved. This is essentially the result proved by Pollard in Ref. 2. Pollard states that more generally one can find a d -point transform for $m = p_1^{n_1} \dots p_t^{n_t}$ if $d \mid (p_i - 1)$ for all i ($i = 1, \dots, t$) and d is the order Mod m .

Bonneau in Ref. 6 has proved a converse of Pollard's result which we restate and prove here in our terminology.

Theorem.

If R_m has a d -point transform and $m = p_1^{n_1} \dots p_t^{n_t}$, m odd, then $d \mid p_i - 1$ for all i and there exists an element $r \in R_m$ such that r is of order d in $R_{p_i^{n_i}}$ for all i .

Proof.

Since R_m has a d -point transform, the delta function, given by (32), must exist where here $m = p_1^{n_1} \dots p_t^{n_t}$. For the inverse transform to exist the inverse $(d)^{-1}$ of (d) , the residue of d Mod m must exist. To find this inverse it is necessary the $(d, m) = 1$; d and m are relatively prime. But this implies $(d, p_i) = 1$ for each i ($i = 1, 2, \dots, t$).

Consider the mapping ψ of ring R_m on to the direct product of rings, $R_{p_1^{n_1}}, R_{p_2^{n_2}}, \dots, R_{p_t^{n_t}}$, i.e.,

$$\psi : R_m \rightarrow \prod_{i=1}^t R_{p_i^{n_i}}$$

which explicitly is

$$\psi(x) = (x \bmod p_1^{n_1}, x \bmod p_2^{n_2}, \dots, x \bmod p_t^{n_t}) \quad (38)$$

where $x \in R_m$. By the Chinese remainder theorem (Ref. 7, pp. 94-95), $\psi(x)$ is a one-to-one mapping. Since $\psi(x + y) = \psi(x) + \psi(y)$ and $\psi(xy) = \psi(x) \cdot \psi(y)$, $\psi(x)$ maps ring R_m onto ring $\prod_{i=1}^t R_{p_i^{n_i}}$ isomorphically.

The set R_m^* of elements relatively prime to m is an Abelian group. $\psi(x)$ maps group R_m^* onto the direct product of cyclic groups $R_{p_i^{n_i}}^*$, isomorphically. That is,

$$R_m^* \simeq \prod_{i=1}^t R_{p_i^{n_i}}^* \quad (39)$$

The order of R_m^* in the isomorphism (39) is the number of elements relatively prime to m , namely the number,

$$\varphi(m) = \prod_{i=1}^r (p_i - 1) p_i^{n_i-1}$$

whereas the number of elements in the cyclic group $R_{p_i}^* n_i$ is

$$\varphi(p_i^{n_i}) = (p_i - 1) p_i^{n_i-1}.$$

In order to have the delta function (32), an element $r \in R_m^*$ of order d must exist, i.e.,

$$r^d = 1.$$

Since $r \cdot r^{d-1} = 1$, the inverse of r exists and equals r^{d-1} . But by an elementary theorem on congruences such an inverse exists if and only if $(r, m) = 1$. This implies $r \in R_m^*$. Since the order of an element of a group divides the order of the group, $d | \varphi(m)$ or

$$d \left| \prod_{i=1}^t (p_i - 1) p_i^{n_i-1} \right|. \quad (40)$$

But by an argument above $(d, p_i) = 1$ for all i . This with (40) yields

$$d \left| \prod_{i=1}^t (p_i - 1) \right|.$$

In order to have a delta function it is necessary that sum s_m satisfy,

$$s_m = \sum_{k=0}^{d-1} (r^m)^k \equiv 0 \pmod{m}$$

for $(m = 1, 2, \dots, d-1)$. Since $m = \pi p_i^{n_i}$ and the $p_i^{n_i}$ are all relatively prime, then

$$s_m = \sum_{k=0}^{d-1} (r^m)^k \equiv 0 \pmod{p_i^{n_i}} \quad (41)$$

for $(i = 1, 2, \dots, t)$ and $(m = 1, 2, \dots, d-1)$.

Now mapping $\psi(x)$ in (38) sends $r \in R_m^*$ into the following vector

$$\begin{aligned} \psi(r) &= (r \bmod p_1^{n_1}, r \bmod p_2^{n_2}, \dots, r \bmod p_t^{n_t}) \\ &= (r_1, r_2, \dots, r_t) \end{aligned}$$

where r_i denotes the residue of r in $R_{p_i}^* n_i$. Consider now the order of r_i in $R_{p_i}^* n_i$. Let this order be d_i so that $r_i^{d_i} = 1$. Evidently d_i must at least divide d so that $d_i \leq d$.

Now suppose $d_i < d$. Then

$$\sum_{k=0}^{d-1} (r_i^{d_i})^k \equiv \sum_{k=0}^{d-1} (r_i^{d_i})^k \equiv \overbrace{1 + 1 + \dots + 1}^{d \text{ times}} = d \pmod{p_i^{n_i}}.$$

But, a previous argument above, $(d, p_i) = 1$ for $i = 1, 2, \dots, t$. Thus (41) for $m = d_i$ satisfies

$$S_{d_i} \equiv d \not\equiv 0 \pmod{p_i^{n_i}}.$$

This is a contradiction to (41). Thus the "projection" r_i of r in $R_{p_i^{n_i}}$ has order d for $i = 1, 2, \dots, t$. But again since the order of an element divides the order of the group,

$$d \mid (p_i - 1) p_i^{n_i - 1}$$

for all i ($i = 1, 2, \dots, t$). Finally, since d and p_i are relatively prime, all i , $d \mid (p_i - 1)$ for ($i = 1, 2, \dots, t$). This proves the converse of Pollard's theorem.

The mapping $\psi(x)$ given by (38) represents an integer modulo m as a vector of residues of relatively prime moduli. The arithmetic associated with this representation has come to be known as modular arithmetic. Also the rings associated with the mapping $\psi(x)$ in (38) are called modular arithmetic rings. Hence it is reasonable to call transforms of type (1), which are mapped by $\psi(x)$ into a modular arithmetic ring, modular arithmetic transforms.

REFERENCES

1. C. M. Rader, "Discrete Convolution via Mersenne Transforms," IEEE Trans. Computers C-21 (December 1972).
2. J. M. Pollard, "The Fast Fourier Transform in a Finite Field," Mathematics of Computation 25 (April 1971).
3. I. S. Reed and G. Solomon, "A Decoding Procedure for Polynomial Codes," Group Report 47.24, Lincoln Laboratory, M.I.T. (6 March 1959), ASTIA No. 24-1701.
4. R. C. Agarwal and C. S. Burrus, "Fast Digital Convolution Using Fermat Transforms," Southwestern IEEE Conf. Record, April 4-6, 1972.
5. I. M. Vinogradov, Elements of Number Theory (Dover Publications, New York, 1954).
6. R. J. Bonneau, "A Class of Finite Computation Structure Supporting a Fast Fourier Transform," MAC Technical Memorandum 31 (Project MAC), M.I.T. (March 1973).
7. G. H. Hardy and E. M. Wright, The Theory of Numbers (Clarendon Press, Oxford, 1954).

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER ESD-TR-75-241	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) The Use of Finite Fields and Rings to Compute Convolutions		5. TYPE OF REPORT & PERIOD COVERED Technical Note
		6. PERFORMING ORG. REPORT NUMBER Technical Note 1975-50
7. AUTHOR(s) Irving S. Reed		8. CONTRACT OR GRANT NUMBER(s) F19628-73-C-0002
9. PERFORMING ORGANIZATION NAME AND ADDRESS Lincoln Laboratory, M.I.T. P.O. Box 73 Lexington, MA 02173		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Program Element 62706E ARPA Order 2006
11. CONTROLLING OFFICE NAME AND ADDRESS Advanced Research Projects Agency 1400 Wilson Boulevard Arlington, VA 22209		12. REPORT DATE 6 June 1975
		13. NUMBER OF PAGES 26
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) Electronic Systems Division Hanscom AFB Bedford, MA 01731		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES None		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) integer transforms fast Fourier transforms convolution digital filters finite fields rings		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This note extends briefly the integer transforms of C.M. Rader (1972) to transforms over finite fields and rings. These transforms have direct application to digital filters and make possible digital filtering without round-off error. In some cases, the parameters of such number-theoretic transforms can be chosen so that substantial reductions in hardware are possible over what would be needed using classical digital filtering techniques.		

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)